סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום (Best Practices) מניעה והתמודדות כנגד חטיפת BGP

סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום (Best Practices)

מניעה והתמודדות כנגד חטיפת BGP

יולי 2020

יולי 2020

תוכן עניינים

מניעה והתמודדות כנגד חטיפת BGP

1. מבוא (Introduction)

פרוטוקול BGP (Border Gateway Protocol) הינו פרוטוקול ניתוב, המהווה את ליבת מערכת הניתוב של רשת האינטרנט[1].
לכל יחידה ניהולית (AS - Autonomous System) לניהול רשת באינטרנט, דוגמת ספק אינטרנט או ארגון גדול, מוקצה מספר מזהה ייחודי (ASN - Autonomous System Number[2]), אשר הינו חלק בלתי נפרד מחוקי הניתוב מאותה יחידה ניהולית אל/מ רשת האינטרנט.
כל AS מהווה צומת ניתוב (וצומת קבלת החלטות עצמאית) אשר עושה שימוש בפרוטוקול BGP לשם בנייה של מסלולי הגישה באופן דינמי, וזאת תוך בחירה של מסלול מועדף בהתאם לפרמטרים שונים, דוגמת AS's אחרים הזמינים למתן שירות, רוחב פס ועלויות.
BGP נמצא בשימוש באינטרנט מאז 1994, בגרסתו הנוכחית (BGP4) מאז שנת 2006 ובבסיסו מורכב משני פרוטוקולים:

א. iBGP (Internal BGP) - פרוטוקול ניתוב בין שני נתבי BGP בתוך אותו AS, כאשר מטרת פרוטוקול זה הינה לספק מידע לנתבים הפנימיים. דוגמא למידע מסוג זה הינו רשימת כתובות IP הנמצאות מחוץ ל-AS.

ב. eBGP (External BGP) - פרוטוקול בין שני נתבי BGP השייכים ל-AS's שכנים (BGP Peers), כאשר מטרת פרוטוקול זה הינה לאתר את המסלול האופטימלי ברשת, וזאת לצד עדכון ה-As's אודות כתובות ה-IP עליהם הוא אחראי, כך שהם ינתבו אליו מידע רלוונטי. **במסמך זה נתמקד בהגנה על פרוטוקול זה.**

ראוי לציין כי פרוטוקול BGP נחשב לעיתים כפרוטוקול ניתוב מסוג מבוסס קשר (Path Vector), אך לעיתים הוא מסווג גם כפרוטוקול המבוסס על מרחק (Distance Vector). הפרוטוקול מתפקד בשכבת האפליקציה של מודל ה-OSI, כלומר, פרוטוקול ה-BGP בונה מסלול שלם לכל ניתוב. כמו כן, כברירת מחדל הפרוטוקול עושה שימוש ב- TCP 179.
במסגרת הפעילות, כל AS מפרסם רשימת תחומי כתובות (Prefix) אליהן הוא יכול להעביר תעבורה. כמו כן, כל AS מאזין לפרסומים מקבילים מצד AS שכנים. ככל

[1] ניתן ללמוד כי ארגונים גדולים, דוגמת ספקי ענן ציבוריים, עושים שימוש ב-BGP לשם ניתוב פנים רשתי, אך על-מנת לפשט את הדיון, מסמך זה מתמקד בניתוב ברשת האינטרנט.
[2] שם חלופי: Number AS

שתחום הכתובות ספציפי יותר, כך הניתוב זוכה לעדיפות כיעד.
לאור זאת נפוץ לראות כי ישנם מצבים שבהם מסלול השליחה של חבילת המידע ליעד שונה ממסלול הקבלה, כאשר יש לזכור כי ברשות כל AS יכולת עצמאית לקביעת מדיניות בהתאם לפרמטרים שונים.
רוצה לומר, BGP הינו פרוטוקול מבוזר; קרי, אין בסיס מידע מרכזי ממנו שואבים כל ה-AS's את מסלולי הניתוב האופטימאליים, וכל AS עשוי לבחור מסלול ניתוב בהתאם למדיניות ומצב הרשת בפועל. סוגיה זו מהותית וזאת לאור העובדה כי טבלאות הניתוב הינן דינמיות ונשמרות בזיכרון הנדיף (RAM) בנתב, ולפיכך פגיעות יותר.
למרות היתרונות הגלומים בפרוטוקול BGP, השימוש בו עשוי לחשוף את הארגון לחטיפת BGP (BGP Hijacking) ; תקיפה שבה תוקף טוען לבעלות על תחומי כתובות IP של הארגון, כך שהוא מסוגל לבצע מניפולציה לתעבורה שמיועדת לארגון. כך לדוגמא, תוקף עשוי ל"כופף" את התעבורה, לשנות את מסלולה כך שהיא תעבור דרך נכס סייבר הנמצא בשליטתו.

2. מטרות ויעדים (Goals & Objectives)

מסמך זה מציג המלצות ליישום לשם מניעה והתמודדות כנגד חטיפת BGP.

3. קהל היעד (Target Audience)

מסמך זה נכתב עבור מנהל הגנת הסייבר בארגון (CISO), מוסמך מתודולוגיות הגנת סייבר, מוסמך מיישם הגנת סייבר, מוסמך טכנולוגיות הגנת סייבר (ארכיטקט הגנה בסייבר), אנשי תקשורת נתונים/תקשוב/IT וסיסטם.
גורמים נוספים אשר עשויים להפיק ערך מוסף ממסמך זה הם מנהל מערכות המידע (CIO - Chief Information Officer), ממונה הגנת הפרטיות (DPO - Data Privacy Officer) וגורמים עסקיים הנדרשים לאשר את הערכת הסיכונים של נכס הסייבר / התהליך העסקי.

4. תיחום המסמך (Scope of This Document)

המסמך "מניעה והתמודדות כנגד חטיפת BGP" מתמקד בהמלצות ליישום לשם מניעה והתמודדות כנגד חטיפת BGP ברשת האינטרנט, וזאת תוך התמקדות

בהגנה על פרוטוקול eBGP.

עם זאת, אין מסמך זה סוקר את כלל ההמלצות לאבטחת פרוטוקול BGP.

כמו כן, ראוי לציין כי המסמך אינו כולל הרחבה בנושאים שלגביהם מערך הסייבר הלאומי כתב ופרסם מסמכים ייעודיים. דוגמה לנושא מסוג זה הינו הגנה פרטנית על מערכת ותשתית, דבר הזוכה למענה במסגרת *'תורת ההגנה בסייבר לארגון'* אשר נכתבה ופורסמה על-ידי מערך הסייבר הלאומי.

5. איומים הנגזרים מחטיפת BGP

פרק זה סוקר את האיומים העיקריים הנגזרים מחטיפת BGP:

	שם האיום	תיאור	מחוללי סייבר שכיחים
1.	מניעת שירות (DOS - Denial of service)	תוקף עשוי ליצור חורים שחורים (Black-Hole) ברשת (האינטרנט), וזאת ע"י יצירת מסלולים כוזבים או באמצעות ביטול מסלולים לגיטימיים.	כשלב מקדים לתקיפה תוקף עשוי להשתמש במחוללים הבאים: א. השתלטות על נתב לגיטימי ופרסום מידע כוזב אודות AS ב. פרסום מסלול קצר יותר (Short Path), כך שנתבים בדרך יעדיפו להעביר את התעבורה דרך נכס סייבר הנמצא בחזקת התוקף
2.	האזנה (Sniffing)	מימוש תקיפה זו מחייב כי התוקף יהיה בעל שליטה על נכס סייבר אשר דרכו תעבורה לגיטימית של הקורבן משונעת. התוקף יכול להשיג זאת ע"י שימוש ב- BGP , וזאת תוך ניתוב תעבורת הקורבן דרך רשת זדונית אשר נמצאת בשליטתו.	
3.	ניתוב תעבורת נכס סייבר	הצעד הראשון בתקיפה זו הוא ביצוע חטיפת BGP,	

	שם האיום	תיאור	מחוללי סייבר שכיחים
	לגיטימית דרך רשת זדונית (Routing to Endpoints in Malicious Networks)	ולאחר מכן הפנייה של תעבורה לגיטימית של נכס הסייבר, לעבר נכס סייבר זדוני (דוגמת אתר Web). באמצעות חזרה על צעדים אלו התוקף יכול להסתיר את פעילותו הזדונית במרחב הסייבר.	ג. פרסום מתחם כתובות (Prefix) פרטני יותר, כך שהניתוב יזכה לתיעדוף גבוה יותר ד. התחזות ל-AS לגיטימי, תוך ביצוע פרסום בתדירות גבוהה (לעיתים משולב תקיפת למניעת שירות כנגד הנתב הלגיטימי, וזאת במטרה למנוע מהנתב לבצע פרסום לשאר ה-AS's) כמו כן, יש לתת את הדעת כי איומים מסוג אלו עשויים להתממש עקב טעות אנוש או התרשלות בהחלת הגדרות תצורה.
4.	יצירת חוסר יציבות במסלול (Creation of Route Instabilities)	עומסים חריגים או ביצוע שינויים לא מבוקרים, עשוי להוביל לידי פגיעה ביציבות שדרת הרשת.	
5.	חשיפת טופולוגית רשת (Revelation of Network Topologies)	שכיח לראות כי השותף להיררכית ה-BGP מקבל חשיפה מלאה למסלולים הקיימים ברשת (דוגמת רשת האינטרנט). מידע זה עשוי להיות שימושי עבור ארגוני פשיעה וגורמים זדוניים אחרים.	

טבלה 1: סקירת איומים כנגד BGP ביחס למחוללי סייבר שכיחים

6. המלצות ליישום לשם מניעה והתמודדות עם חטיפת BGP

פרק זה מציג רשימה של המלצות ליישום, אשר מימוש נכון שלהן יסייע למניעה והתמודדות עם חטיפת BGP:

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
המלצות כלליות		
1.	מומלץ לבצע הערכת סיכונים (Risk Assessment)	
2.	מומלץ לוודא כי נתב התקשורת (Router)עושה שימוש בגרסת קושחה (Firmware) ומערכת הפעלה עדכניות.	
3.	מומלץ לוודא כי נעשה שימוש בגרסה עדכנית של פרוטוקול BGP (גרסה 4 נכון לזמן כתיבת מסמך זה).	
4.	מומלץ להחיל את ההמלצות הבאות במטרה להגן על שכבת הניהול (Control Plane) מפני תקיפות מניעת שירות: א. יש לוודא כי קבלת מסרי BGP מתאפשרת רק מנתבים מוכרים/מורשים, וזאת באמצעות החלת רשימת בקרת גישה פרטנית (ACL - Access Control List). ב. יש להפעיל מנגנונים מקובלים לשם החלת מגבלת קצב גישה.(Rate Limit)	
5.	מומלץ לבצע הקשחה ייעודית לנתב באמצעות שימוש ב:	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	Secure router template (platform dependent) Secure bgp template (platform dependent) להרחבה ראו: https://team-cymru.com/community-services/templates/	
6.	מומלץ לוודא כי כרטיסי רשת (Interfaces) של הנתב שאינם בשימוש מנותקים פיזית מהרשת, ונמצאים במצב כבוי (Shutdown).	
7.	מומלץ לבצע סריקת פורטים עיתית מהאינטרנט על-מנת לוודא כי אין חשיפה שלא לצורך של: א. פורט TCP 179 בו עושה שימוש פרוטוקול ה-BGP. ב. ממשקי הניהול של הנתב (דוגמת SSH, HTTP/S).	
המלצות פרטניות לנושא BGP		
8.	מומלץ להגביל את מספר תחומי הכתובות אשר ניתן לקבל מנתב שכן, כאשר לאחר איתור חריגה יש לסגור את הפעילות (Session) מול השכן.	
9.	מומלץ להחיל סינון כך שרק תחומי כתובות מוכרות/מורשות ניתן יהיה לקבל/לשלוח, וזאת תוך ביצוע קורלציה ל-AS המתאים.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	עם זאת, יש לתת את הדעת כי עקב אילוצים תפעוליים מימוש סינון פרסומי כתובות נכנס/יוצא עשוי להיות ממומש באופנים שונים.	
10.	מומלץ להשוות את ה-TTL של מסרי ה-BGP המתקבלים, וזאת ביחס לערך TTL אשר הוגדר מראש, כך שניתן יהיה לגלות, לזהות ולסכל מסרים חריגים, אשר עשויים להעיד על שינוי לא רצוני במספר ה-Hop בתווך. עם זאת, מומלץ לבחון בקפידה האם לבצע אכיפה אוטומטית או להסתפק בניטור, ובהתאם לממצאי התחקור לבצע אכיפה בפועל.	
11.	מומלץ לוודא כי קבלת מסרי BGP ועיבודם מותנית בהשלמת הליך אימות באופן מוצלח בין הנתבים השכנים. שכיח כי פרוטוקול BGP מאפשר שימוש במספר מנגנוני אימות: א. אימות מבוסס סיסמה משותפת (דוגמת HMAC-MD5 או HMAC-SHA1-12). שיטת אימות זו נחשבת לחלשה, והיא לא מאפשרת אימות מקצה לקצה של כל ה-AS's בתהליך, ובכל מקרה היא מוודאת רק את זהות הנתב השכן, ולא את נכונות המידע המתקבל ממנו. ב. RPKI (Resource Public Key Infrastructure) - אימות על בסיס ארכיטקטורת מפתח פרטי/ציבורי, אשר מטרתו לוודא את מסר ה BGP כנגד מנגנון שרשרת של אמון (Chain of Trust), בדומה לתעודות דיגיטליות של אתרי אינטרנט. מנגנון זה מוודא את הקשר בין ASNs וטווחי	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	כתובות לבין בעליהן. המנגנון לא דורש שכל שכן דרכו עובר מסר ה BGP יתמוך ויממש RPKI. על מנת לממש מנגנון זה נדרשת תוכנה צד שלישי, אליה פונה הנתב על מנת לוודא את אמינות המידע. לשם שיפור רמת האבטחה, RPKI מאפשר להגדיר מהו האורך המינימלי של מתחם כתובות שניתן לקבל משכן. ג. BGPsec - במסגרת תהליך האימות נעשה שימוש ב-RPKI, ובנוסף מתבצע הליך לוידוא נכונות ה Path של ה-AS המקבל, לזה שמפרסם את טווח כתובות ה IP. החתימה והיכולת לוודא אותה הינם הרחבה לפרוטוקול ה BGP, ועל מנת שניתן יהיה לעשות שימוש אפקטיבי ב BGPsec נדרש שכל שכן BGP בדרך בין נותן השירות למקבל יתמוך ב BGPsec. שיטת אימות זו נחשבת לחזקה, והיא מאפשרת אימות מקצה לקצה של כל ה-AS's בהיררכיה. עם זאת, שיטת אימות מאתגרת יותר למימוש, והיא עשויה לדרוש משאבי עיבוד גבוהים יותר (CPU High Usage) מהנתבים בהיררכיה.	
12.	מומלץ לבצע בקרה רציפה ומתמשכת (Continuous Monitoring) לטופולוגית ה-BGP והמסרים המתקבלים (לרבות הודעות שגיאה), וזאת לשם גילוי וזיהוי שינויים לא מורשים, ונקיטה בפעולות מתקנות בהתאם לצורך. שכיח כי מימוש המלצה זו מחייב שילוב פתרון ניטור צד-שלישי, המשקף לארגון את מצבו ביחס לעולם.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.13	מומלץ לקבל התראות מ-AS's שכנים לתיבת דוא"ל מנוטרת, וזאת לשם קבלת מידע אודות שגיאות או שינויים לא מבוקרים, ובהתאם לצורך, נקיטה בפעולות מתקנות.	
.14	מומלץ לוודא כי נוהל התגובה לאירועי סייבר כולל התייחסות לנושא התמודדות עם חטיפת BGP.	
.15	מומלץ לוודא כי הארגון מתרגל באופן עתי התמודדות עם תרחישים הרלוונטיים לחטיפת BGP.	
שרשרת האספקה		
.16	מומלץ לעגן מול הגורמים הרלוונטיים בשרשרת האספקה (דוגמת ספק האינטרנט) דרישה כי היררכית ה-BGP תידרש לעמוד בהמלצות מסמך זה. דבר זה נכון אף לארגונים שאינם בעלי AS עצמאי.	
.17	מומלץ לוודא כי ספקי השירות הרלוונטיים עומדים בדרישות מתודת שרשרת האספקה[3] של המערך.	

טבלה 2: המלצות ליישום לשם מניעה והתמודדות עם חטיפת BGP

[3] שאלון ספקים לחיזוק שרשרת האספקה
https://www.gov.il/he/departments/news/querysupply

1. נספחים (Appendixes)

פרק זה מכיל את רשימת הנספחים הנלווים למסמך זה.

נספח 1 - מניעה והתמודדות כנגד חטיפת BGP

מטרת הנספח

לשקף לקורא את אופן פיתוח המסמך, הגורמים המעורבים בתהליך כתיבתו ובהעברת משוב על התכנים לטובת מתן שקיפות וגילוי נאות לתהליך ולגורמים המעורבים על סוגיהם.

א. כיצד גובש המסמך - סקר שוק/סילבוס/השוואה בעולם

1) בחינה של תיעוד/תקינה מהעולם כגון NIST, ISO, ועוד (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
2) בחינה של פרסומים מקובלים בתחום (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
3) שיח עם איגוד האינטרנט הישראלי.

2. קיצורי שמות (Acronyms)

פרק מציג את קיצורי השמות בהם נעשה במסמך זה.

שם המונח	ביאור
דוא"ל	דואר אלקטרוני
ACL	Access Control List
AS	Autonomous System
ASN	Autonomous System Number
BGP	Border Gateway Protocol
CPU	Central Processing Unit
eBGP	External\Exterior BGP
DoS	Denial of Service
HMAC	Hash-Based Message Authentication Code
iBGP	Internal\Interior BGP
IPS	Intrusion Prevention System
MD	Message-Digest
MiTM	Man-in-the-Middle Attack
OSI	Open Systems Interconnection
SHA 1	Secure Hashing Algorithm 1
RIR	Regional Internet Registry
RPKI	Resource Public Key Infrastructure
TTL	Time to Live

טבלה 3: קיצורי השמות בהם נעשה שימוש במסמך זה

3. מסמכים ישימים (Applicable Documents)

פרק זה מכיל את מקורות המידע עליהם הסתמכו הכותבים בעת כתיבת המסמך.

מקורות מידע בעברית:

מערך הסייבר הלאומי

המלצות ליישום - הקשחת מערכות מחשוב

- ✓ https://www.gov.il/he/departments/general/systemhardening

שימוש בשירותי ענן - הרחבה לתורת ההגנה בסייבר לארגון

- ✓ https://www.gov.il/he/departments/policies/cloud_services

תורת ההגנה בסייבר לארגון

- ✓ https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר

- ✓ https://www.gov.il/he/Departments/news/cybercrisispreparedness

שאלון ספקים לחיזוק שרשרת האספקה

- ✓ https://www.gov.il/he/departments/news/querysupply

כללי

BGP Hijacking או עד כמה קל להפיל את האינטרנט?, דן פייגין, Digital Whisper, גליון 102, ינואר 2019

- ✓ https://www.digitalwhisper.co.il/files/Zines/0x66/DW102-1-BGPHijacking.pdf

על שתי שיטות ל־BGP Security הדרגתי, עופר שכטר, האוניברסיטה העברית

- ✓ https://www.cse.huji.ac.il/~omershe/notes/bgp.pdf

מקורות מידע באנגלית:

General

Securing BGP

- ✓ https://rpki.readthedocs.io/en/latest/rpki/securing-bgp.html

BOGON ROUTE SERVER PROJECT

- ✓ https://team-cymru.com/community-services/bogon-reference/bogon-reference-bgp/

Chapter 21 - Network Attack & Defense, Galit Balmas, Haifa University, 2014

- ✓ http://www.cs.haifa.ac.il/~orrd/CompSecSeminar/2014/GalitBalmas-Chapter21.pdf

Are We There Yet? On RPKI's Deployment and Security

- ✓ https://eprint.iacr.org/2016/1010.pdf

DISCO: Sidestepping RPKI's Deployment Barriers

- ✓ https://www.cse.huji.ac.il/~schapiram/hlavacek20ndss-disco.pdf

A Guide to Border Gateway Protocol (BGP) Best Practices, NSA, 27 August, 2018

- ✓ https://apps.nsa.gov/iaarchive/library/reports/a-guide-to-border-gateway-protocol-bgp-best-practices.cfm

SP 1800-14 NIST Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation

- ✓ https://csrc.nist.gov/publications/detail/sp/1800-14/final

Improving BGP routing security by minding your MANRS

- ✓ https://www.csoonline.com/article/3433263/improving-bgp-routing-

security-by-minding-your-manrs.html

FINAL Report - BGP Security Best Practices, CSRIC, March, 2013

- ✓ https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

BGP ROUTE HIJACKING

- ✓ https://blogs.akamai.com/2018/11/bgp-route-hijacking.html

Cisco

Types of BGP Attacks

- ✓ https://www.ciscopress.com/articles/article.asp?p=1237179&seqNum=2

Protecting Border Gateway Protocol for the Enterprise

- ✓ https://tools.cisco.com/security/center/resources/protecting_border_gateway_protocol

MANRS

MANRS for Network Operators

- ✓ https://www.manrs.org/isps/

MANRS Implementation Guide

- ✓ https://www.manrs.org/isps/guide/antispoofing/

IETF

BGP Operations and Security, RFC 7454

- ✓ https://tools.ietf.org/html/rfc7454

Using RPSL in Practice, RFC 2650

- ✓ https://tools.ietf.org/html/rfc2650

***** סוף מסמך *****